ABSTRACT OF THE DISCLOSURE

Methods for securing booting a personal computer system. One method includes establishing a secret between two or more devices and securing the secret in each of the two or more devices. Another method includes processing BIOS code instructions and accessing security hardware. The method also includes accessing a first device, locking the security hardware, and calling boot code. Another method includes reading a secret from a first location, storing the secret in a secure location different from the first location, and locking the first location. Another method includes requesting authentication for a device, receiving authentication for the device, and setting a timer associated with the device. Another method includes requesting authentication for a device, failing authentication for the device, and preventing access to the device upon failing authentication for the device.